Arnold's proof of the nonexistence of a solution to the quintic equation

Identity, Maths Club of IISER Kolkata

Indian Institute of Science Education and Research Kolkata

November 23, 2022

Gadadhar Misra
Indian Statistical Institute Bangalore
And
Indian Institute of Technology Gandhinagar

Square roots

Here is a proof that $\sqrt{2}$ is not rational.

Suppose to the contrary that $\sqrt{2} = \frac{p}{q}$ without any common factors.

Then $\sqrt{2} = \frac{2q-p}{p-q}$ but with a smaller denominator leading to a contradiction.

For $n \geqslant 3$, $\sqrt[n]{2}$ is not rational either. If not, as before, we must have

$$p^n = 2q^n = q^n + q^n$$

for a pair of integer p and q. But this contradicts the Fermat's last theorem!

$\sqrt{2}$ and $-\sqrt{2}$ can't be algebraically distinguished, that is, if $\sqrt{2}$ is the solution of a polynomial equation with rational coefficients, then so is $-\sqrt{2}$ and vice-versa. Such pairs are called conjugate.

More generally, two real numbers a and b are conjugate over $\mathbb{Q}$ if for all polynomials p with coefficients in $\mathbb{Q}$,

$$p(a) = 0 \iff p(b) = 0.$$

Similarly, two complex numbers z, z' are said to be conjugate if for all polynomials with coefficients in $\mathbb{R}$

$$p(z) = 0 \iff p(z') = 0.$$

The two numbers i and $-i$ are indistinguishable.

Definition: Let $k \geq 0$, and let $\left(z_1, \ldots, z_k\right)$, $\left(z_1', \ldots, z_k'\right)$ be $k-$tuples of complex numbers. Then $\left(z_1, \ldots, z_k\right)$ and $\left(z_1', \ldots, z_k'\right)$ are conjugate over $\mathbb{Q}$ if for all polynomials p over $\mathbb{Q}$ in k variables

$$p\left(z_1, \ldots, z_k\right) = 0 \iff p\left(z_1', \ldots, z_k'\right) = 0.$$

The symmetry group of a polynomial: Write $(s_1, \ldots, s_k)$ for its distinct solutions in $\mathbb{C}$. The Galois group of p is

$\mathrm{Gal}(p) = \left\{\sigma \in S_k : \left(s_1, \ldots, s_k\right) \textit{ and } \left(s_{\sigma(1)}, \ldots, s_{\sigma(k)}\right)\right.$ are conjugate$\}$

'Distinct solutions' means that we ignore any repetition of roots: if $p(t) = t^5(t-1)^9$, then $k = 2$ and $\left\{s_1, s_2\right\} = \{0,1\}$.

Informally, let us say that a complex number is radical if it can be obtained from the rationals using only the usual arithmetic operations and kth roots. For example, $\dfrac{\frac{1}{2} + \sqrt[3]{\sqrt[5]{2} - \sqrt[2]{7}}}{\sqrt[4]{6 + \sqrt[3]{\frac{2}{3}}}}$ is radical, whichever square root, cube root, etc., we choose. A polynomial over $\mathbb{Q}$ is solvable (or soluble) by radicals if all of its complex roots are radical.

Every quadratic over $\mathbb{Q}$ is solvable by radicals. This follows from the quadratic formula: $\frac{1}{2a}\left(-b \pm \sqrt{b^2 - 4ac}\right)$ is visibly a radical number.

Theorem of Galois

What determines if a polynomial is solvable by radicals? The amazing answer to this question was given by Galois.

Theorem: Suppose that p is a polynomial over $\mathbb{Q}$. Then p is solvable by radicals if and only if the Galois group $\mathrm{Gal}(p)$ is solvable.

We are going to however, discuss an elementary (by no means, trivial) proof due to Arnold.

Solution of polynomial equations

Let $p(z) = z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0$ be a polynomial with complex coefficients $c_{n-1}, \ldots, c_0$. By the fundamental theorem of algebra, there are exactly n solutions to the equation $p(z) = 0$, say, $\{s_1, \ldots, s_n\}$. What happens to the solutions $\{s_1, \ldots, s_n\}$ if we move the coefficients $c_{n-1}, \ldots, c_0$ a little and what happens the other way around?

The answer involves permutations, loops, roots (of complex numbers), finally commutators.

It is clear that given a set of complex numbers $S = \{s_1, \ldots, s_n\}$, the set of solutions of

$$p(z) = 0, \text{ where } p(z) = (z - s_1)\cdots(z - s_n),$$

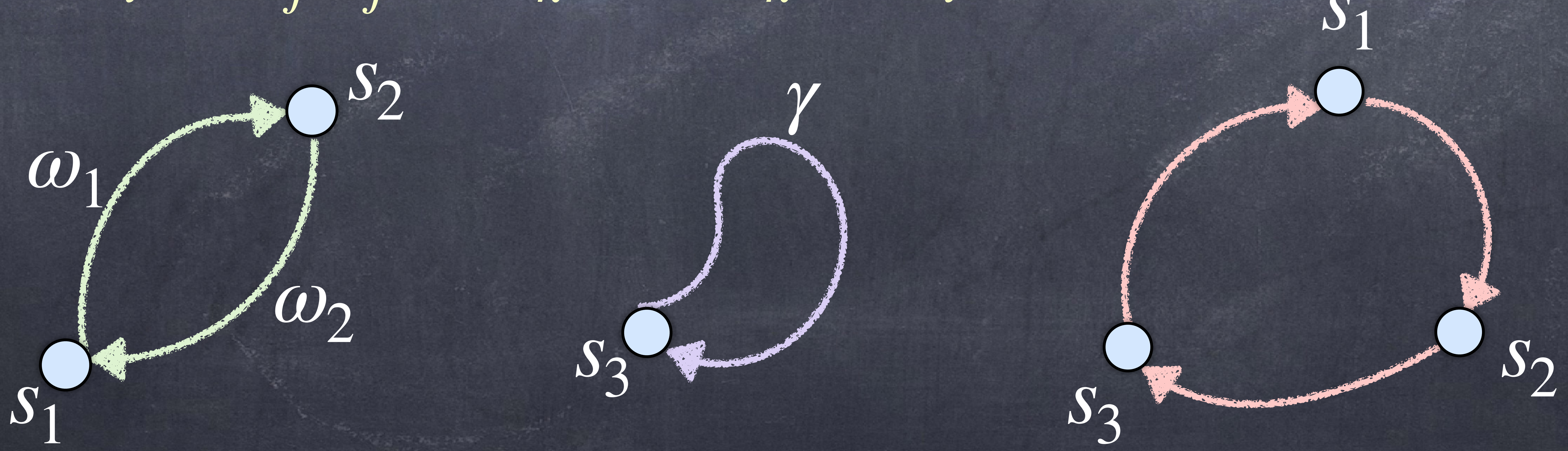
is exactly S. It is going the other way round, that is, how to find the solutions of a polynomial equation is not obvious.

Two kinds of permutations

We discuss two kinds of permutations, namely, transpositions and cycle:

- transpositions, denoted (ij), exchanging the position of two solutions, i.e., $s_i \to s_j$.

- cycles, denoted (ijk), exchanging the position of three solutions cyclically, i.e., $s_i \to s_j$, $s_j \to s_k$, and $s_k \to s_i$.



Loops and permutations

Locating the solutions $(s_1, \ldots, s_n)$ in $\mathbb{C}$, we can think of a permutation to be a path traveling from one solution to another.

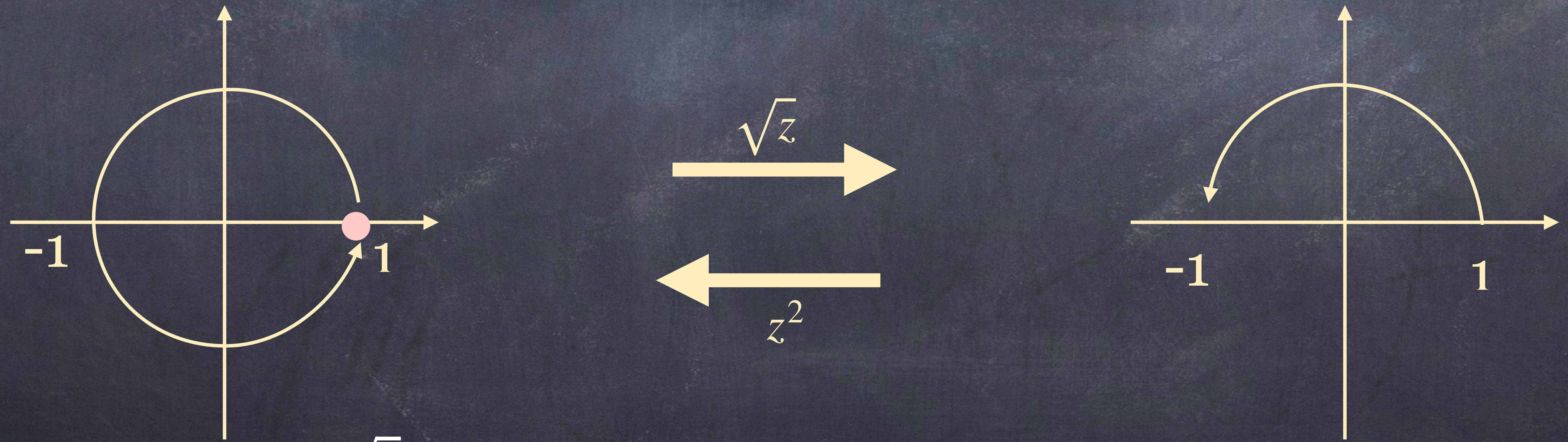
Paths in the complex plane are just continuous curves that connect two points (we assume that they do not self-intersect, otherwise things get unnecessarily complicated).

A path that closes, i.e., connects a point to itself, is called a loop and denoted γ.

These paths will be represented by arrows in all the figures, and will be used to induce permutations on the solutions $(s_1, \ldots, s_n)$.

How complex roots move around in $\mathbb{C}$

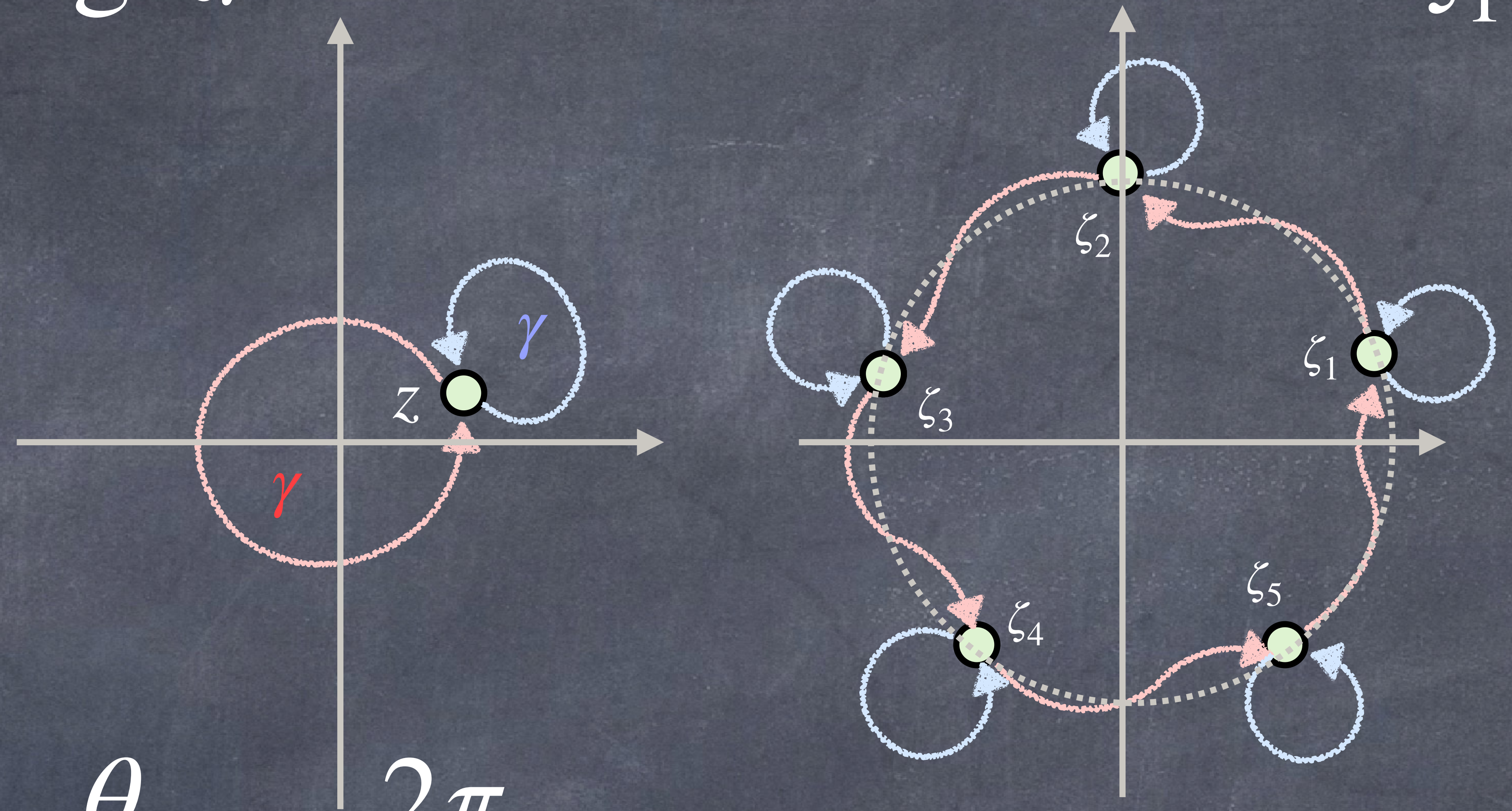
Fixing some complex number z, a root of z is some number ζ in $\mathbb{C}$ such that $\zeta^k = z$for some $k \in \mathbb{N}$. By the fundamental theorem of algebra, there are exactly k such kth root ζ of z; and z. Thus, $\sqrt[k]{z}$ denotes a multivalued function of the complex variable z. With a little abuse of notation, we let $\sqrt[k]{z}$ also denote any of the kth roots of z. Fixing $k \in \mathbb{N}$ and assuming that z itself follows a loop γ, we ask what kind of path $\sqrt[k]{z}$ follows. Notice that with $k = 2$, we have



When z follows a loop γ, $\sqrt{z}$ does not always follow a loop.

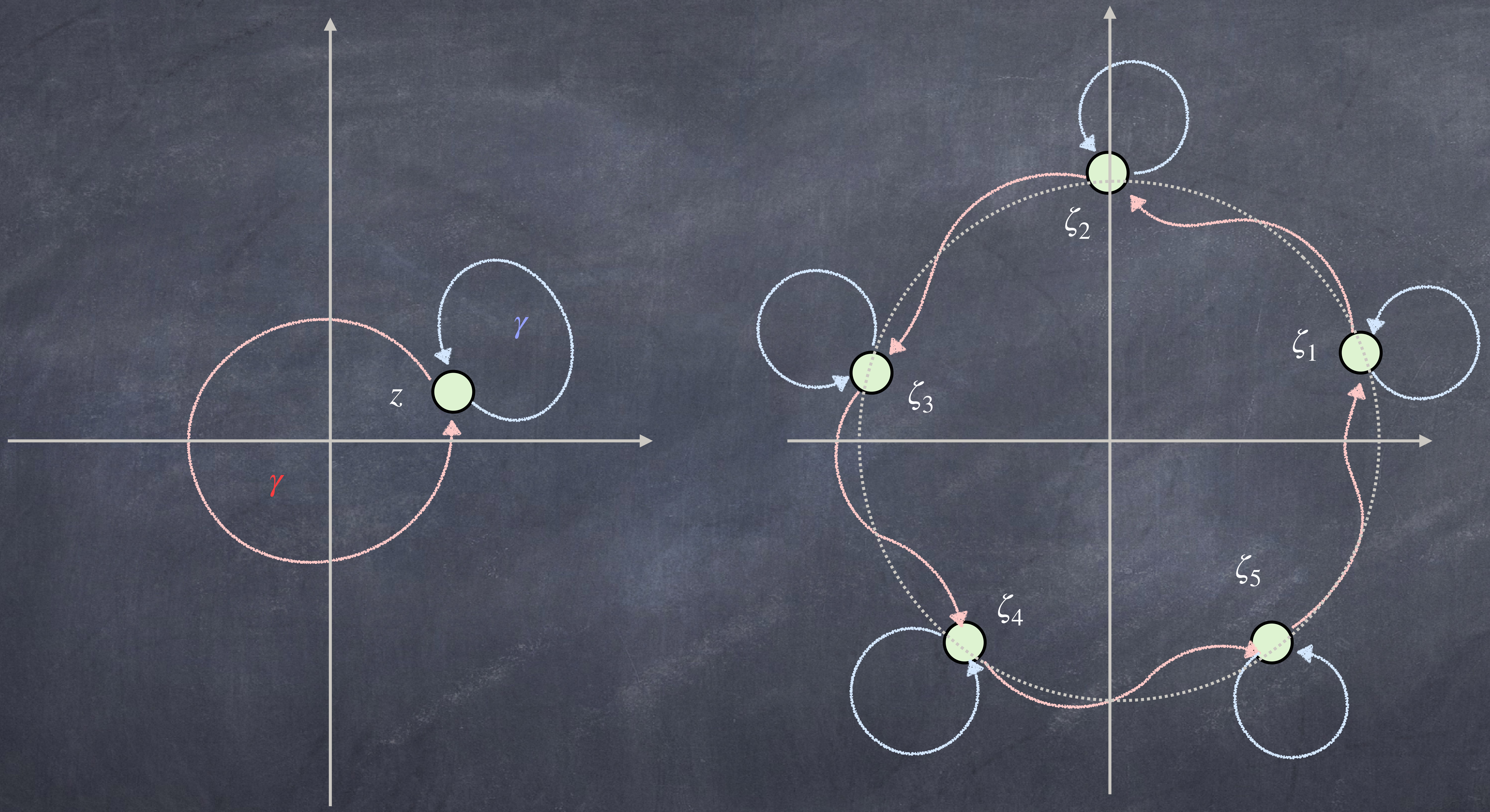
Set $z = re^{i\theta}$ with $r = |z|$ and $\theta = \arg z$, and write the kth roots $\zeta_1, \ldots, \zeta_k$ explicitly as

$$\zeta_\ell = \sqrt[k]{r}e^{i(\theta+2\ell\pi)/k}, \ \ell \in \{1,\ldots,k\}.$$



Thus, the argument $\arg(\zeta_\ell)$ of $\zeta_\ell = \dfrac{\theta}{k} + \ell\dfrac{2\pi}{k}$. This means that all roots are equally spaced on the circle of radius $\sqrt[k]{r}$, at angle $\dfrac{2\pi}{k}$ apart.

As z travels along a path γ, winding once around 0, its kth roots also move around since the $\arg(z)$ has gone from θ to $\theta + 2\pi$. Each kth root ζ_ℓ has moved to its closest, counter clock-wise neighbour $\zeta_{\ell+1}$. In particular, the roots have not completed a loop.



z
γ
γ
ζ_1
ζ_2
ζ_3
ζ_4
ζ_5

A formula for a solution s of a polynomial equation of the form $p(z) = 0$, in general, is of the form $s = R(c_0, c_1, \ldots, c_{n-1})$, where R is some function of the coefficients $c_0, \ldots, c_{n-1}$ of p obtained by using $+, -, \times, \div, \sqrt{\ }$.

A hierarchy of functions: The first ones, say R_0,that are made out of the coefficients $c_0, \ldots, c_{n-1}$ using only $+, -, \times, \div$. These are polynomial, or more generally, rational functions of the coefficients of the polynomial p.

Therefore, if two or more of these coefficients follow a loop the function of type R_0 also follows a loop.

This last property of R_0 functions is not shared by R_1 functions obtained from R_0functions by taking roots, as we have seen.

When $(c_0, \ldots, c_{n-1})$follow a loop, R_1-functions do not necessarily follow a loop.

We can build R_2-functions by taking roots of R_1-functions building higher order of nesting in the coefficients at each stage. Consider for example:

$R_0 = -\frac{c_3}{6}+c_0,$ or $c_2^3 + c_1,$

$R_1 = \sqrt{c_5^2 - 3}+\frac{1}{2}c_4^2 - \sqrt[3]{c_0},$

$R_2 = \sqrt[3]{\frac{2}{3}c_3^2 - c_1} + \sqrt{\frac{1}{3}c_2 + \sqrt[5]{c_5^2 + c_0 - 1}} + c_4, \ldots$

Quadratic Equation

First observation: Coefficients $c_0, c_1, \ldots, c_{n-1}$ are symmetric functions of the solutions $\{s_1, \ldots, s_n\}$. This follows since the polynomial $(z - s_1)\cdots(z - s_n)$ is independent of the ordering of the solutions $\{s_1, \ldots, s_n\}$.

For $n = 2$, if the two solutions s_1, s_2 are permuted using the transposition , the coefficients (c_0, c_1) each move on some path but they must come back to the original position when s_0 and s_1 exchange their position.

Theorem: There is no map $R_0 : \mathbb{C}^2 \to \mathbb{C}$ such that $R_0(c_0, c_1)$ is always a solution to the quadratic equation $p(z) = 0$, where $p(z) = z^2 + c_1 z + c_0$.

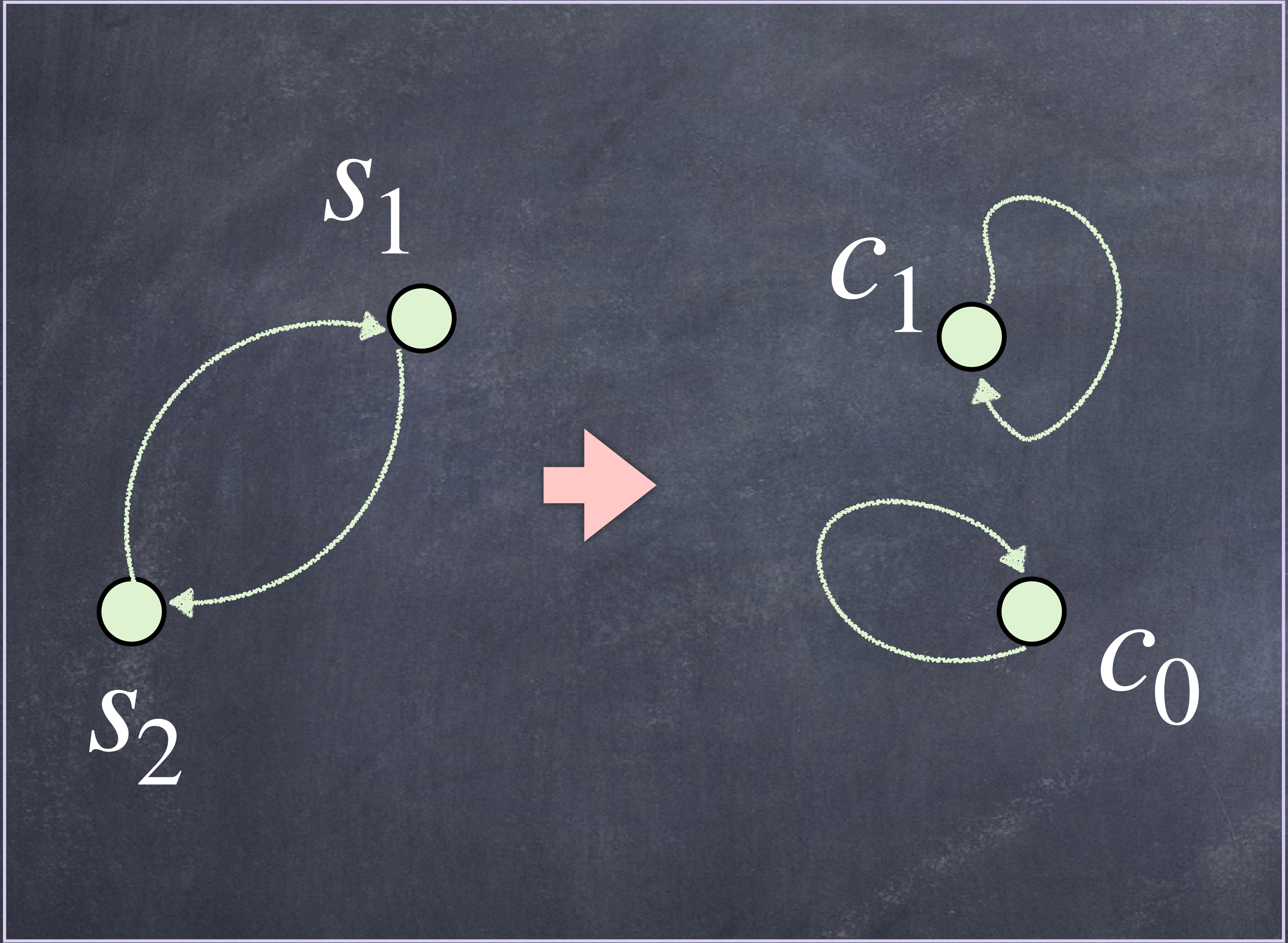
- The transposition (12) swaps the two solutions s_1 and s_2. Pick a continuous path $s_1(t)$ starting at $s_1 := s_1(0)$ and ending at $s_1(1) = s_2 = s_2(0)$. Also, choose a path s_2 starting at $s_2 = s_2(0)$ and ending at $s_2(1) = s_1 = s_1(0)$.

- The coefficients $c_0(t), c_1(t)$ are continuous symmetric functions of the solutions $\{s_1(t), s_2(t)\}$, therefore their final positions are the same as the initial positions. Thus, each c_0, c_1 defines a loop. The functions

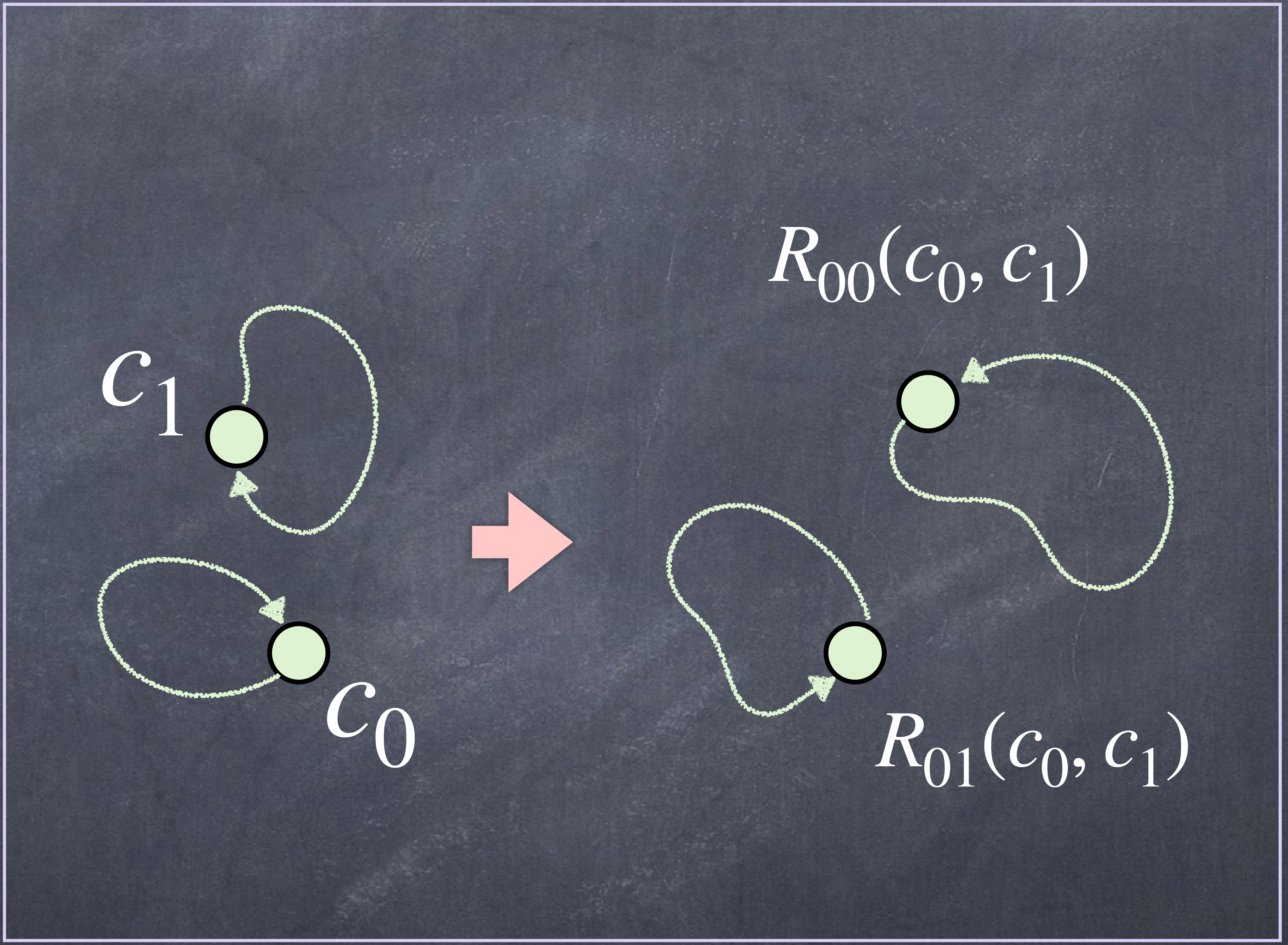
$$R_{0i}(c_0(t), c_1(t)) = s_i(t), \ i = 1,2,$$

being a continuous function of c_0, c_1, by hypothesis, will also follow its own loop.

- Consequently, as t runs from 0 to 1, the solutions s_1 and s_2 swap their positions while $R_{01}(c_0(0), c_1(0))$ and $R_{02}(c_0(1), c_1(1))$ coincide leading to a contradiction.



s_1
s_2
c_1
c_0



c_1
c_0
$R_{00}(c_0, c_1)$
$R_{01}(c_0, c_1)$

The cubic Equation

- Let $p(z) = 0$, where $p(z) = z^3 + c_2z^2 + c_1z + c_0$, be the cubic equation.

- Again, assume that we have solutions of the form

$$s_i = R_{1i}(c_0, c_1, c_2), i = 1,2,3,$$

  involving one level of radicals.

- We still have that each of the coefficients follow a loop as solutions permute.

- However, functions like $R_1$with radicals in them no longer follow a loop.

- We need a new idea!

Commutators

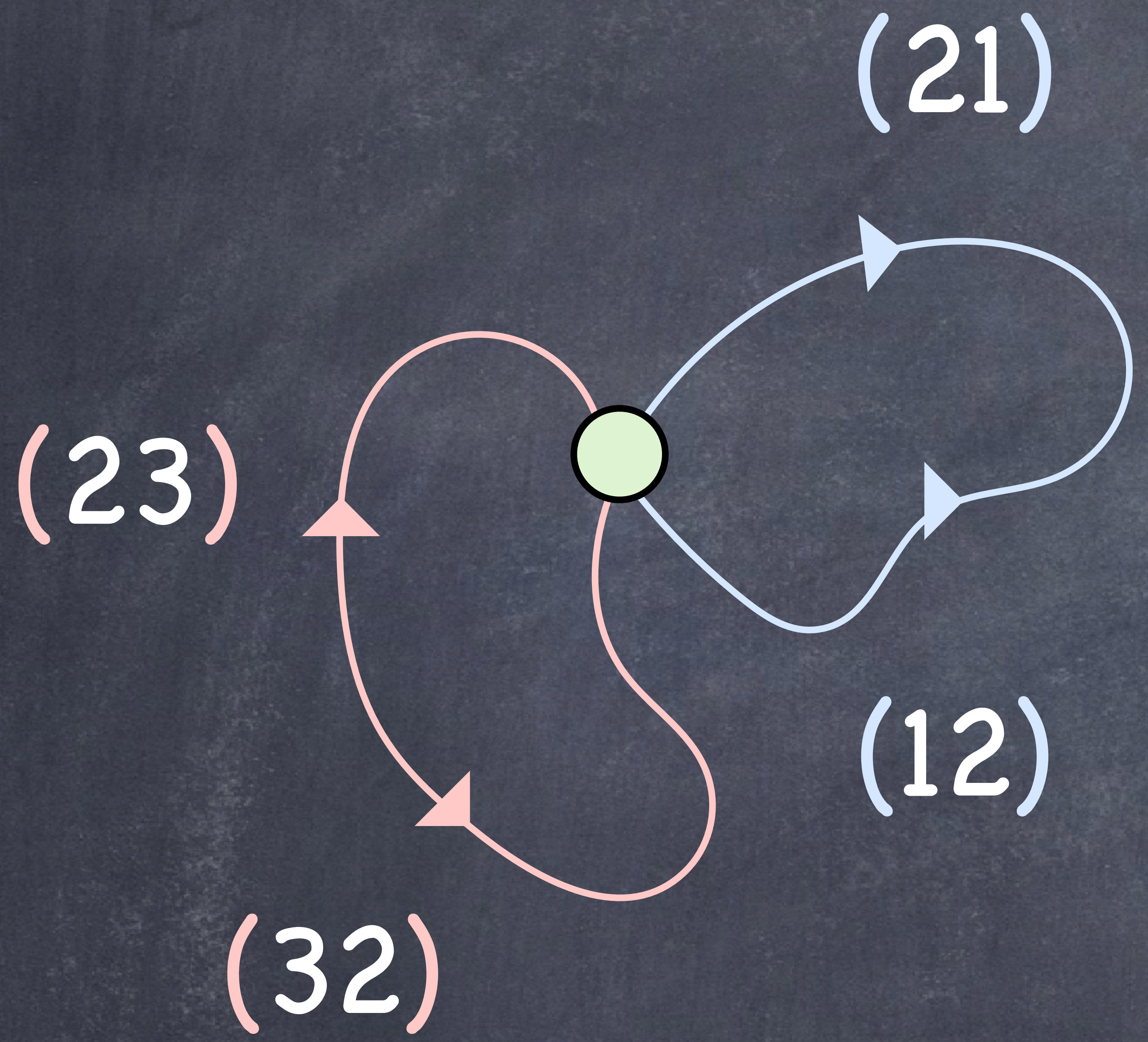
- Consider the transposition (12) that induces a loop $\gamma_1$on R_0 and an unclosed path ω_1 on R_1. Consider also (23), inducing a loop γ_2 on R_0 and a path ω_2 on R_1. Now perform the following sequence of transpositions, called the commutator of (12) and (23), and denoted

$$[(12),(23)] = (12)(23)(12)^{-1}(23)^{-1}.$$

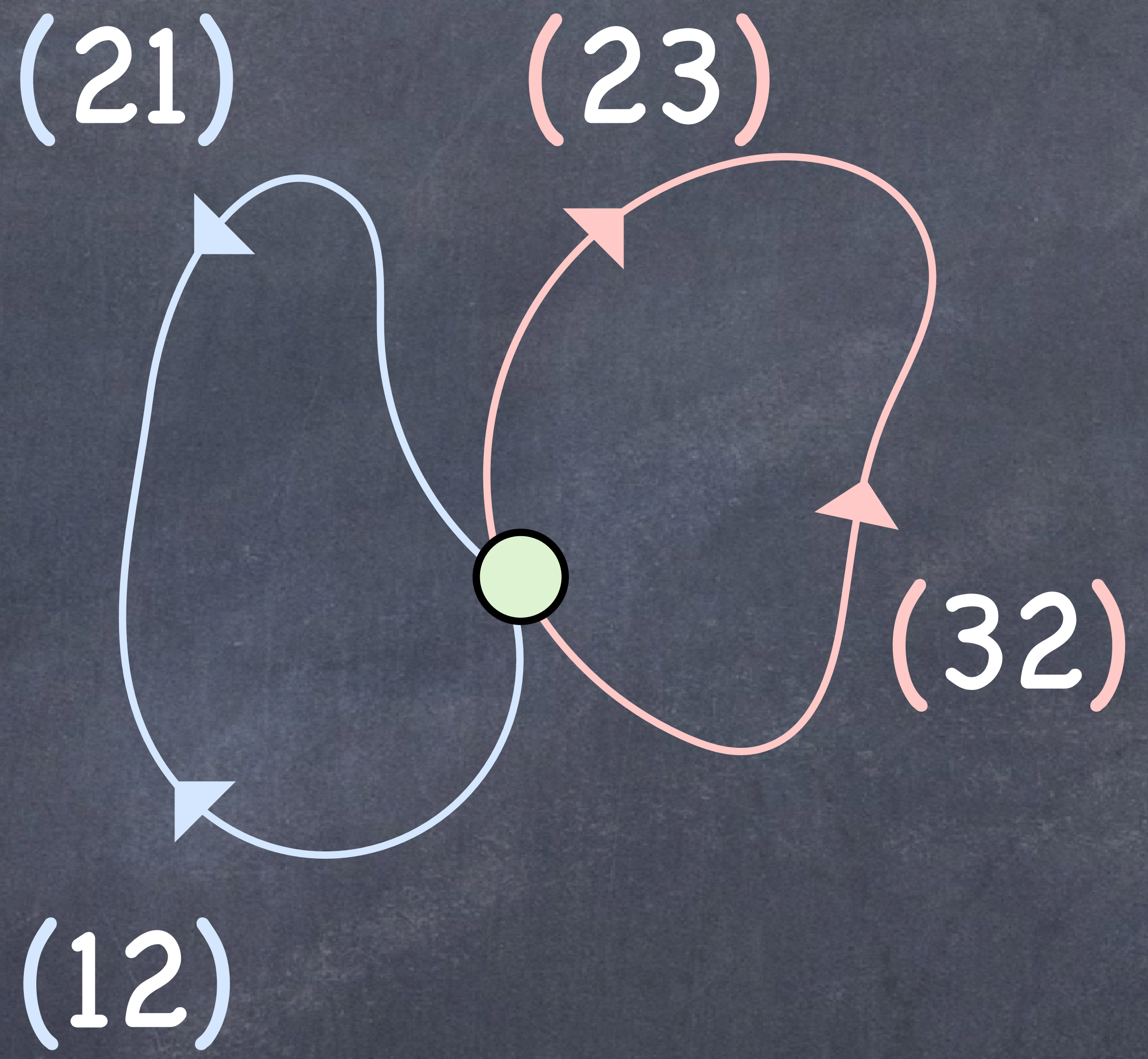
- Since $(12)^{-1}$ is (21), and $(23)^{-1} = (32)$, it follows that $[(12),(23)]$ is the cycle (123). Indeed, this is true of any pair of transposition, namely, $[(ij),(jk)] = (ijk)$.

- Therefore, $[(12),(23)]$ permutes the three solutions $\left(s_1, s_2, s_3\right)$.

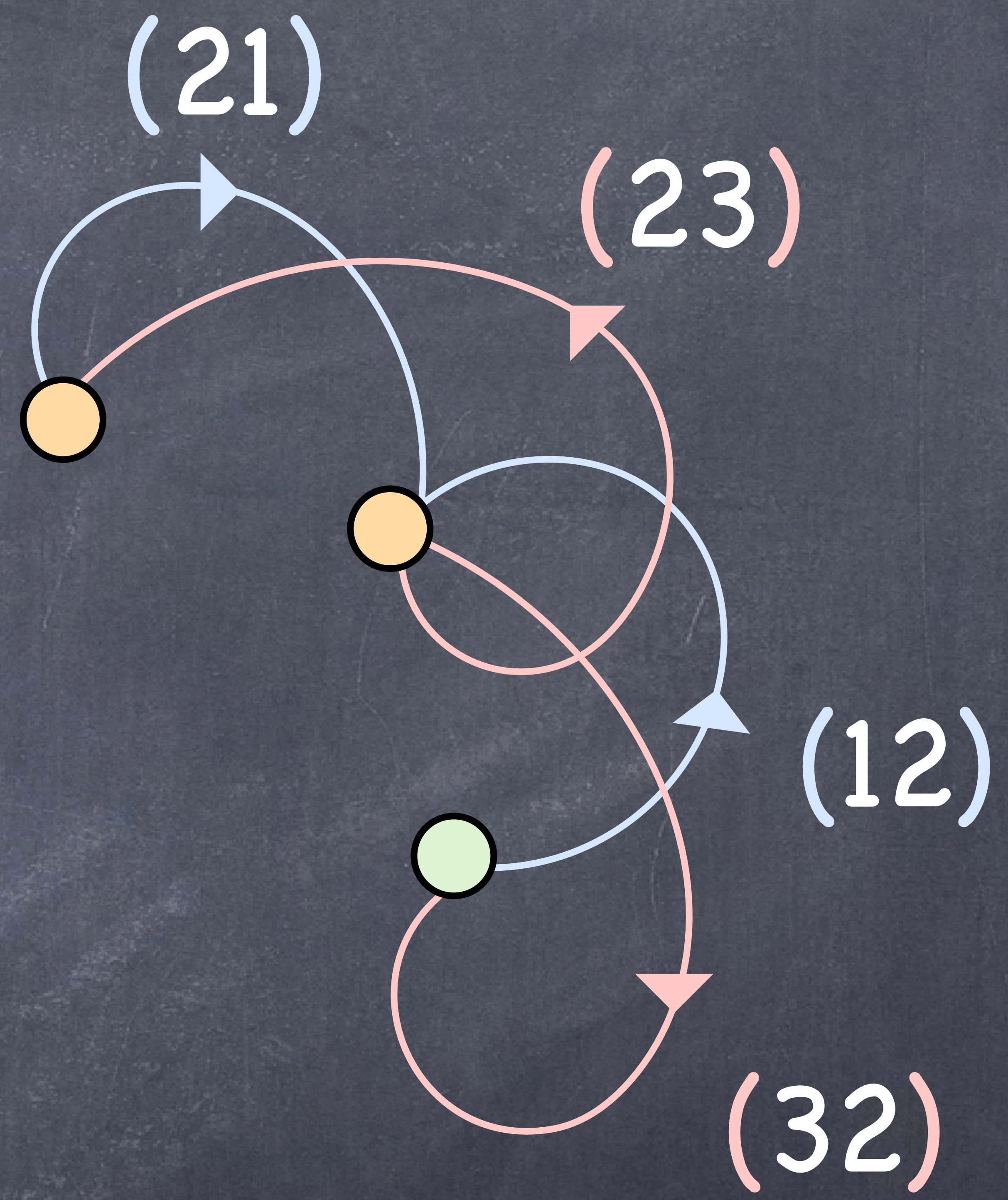
- Now, R_0follows a sequence of loops $\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$, which is itself a loop, however, R_1 follows a sequence of unclosed paths $\omega_1\omega_2\omega_1^{-1}\omega_2^{-1}$ (visiting other roots) but closes on itself by construction.



C



R_0



R_1

- Suppose that (s_1, s_2, s_3) undergoes the permutation (123).
- Then both R_0 and R_1 follow a loop. Consequently, we can't have equalities:

$$s_i = R_{1i}(c_0, c_1, c_2), i = 1,2,3.$$

- Theorem: There is no map $R_1 : \mathbb{C}^3 \to \mathbb{C}$ such that $R_1(c_0, c_1, c_2)$ is always a solution to the cubic equation

$$p(z) = 0, \text{ where } p(z) = z^3 + c_2 z^2 + c_1 z + c_0.$$

The Quartic

- We have seen that solutions of a cubic equation, in general, cannot be written using functions of type R_1 (one level of roots).

- Now, for the quartic equation,

$$p(z) = 0, \text{ where } p(z) = z^4 + c_3 z^3 + c_2 z^2 + c_! z + c_0,$$

- Assume that we have a solution of the form:

$$s_i = R_{2i}(c_0, c_1, c_2, c_3), i = 1,2,3,4,$$

with two levels of the nesting of roots.

The proof consists of constructing an appropriate permutation of the solutions $\{s_1, s_2, s_3, s_4\}$.

- As before, like the method for the quadratic did not work for the cubic, the method for the cubic doesn't really work for the quartic.

- Hunt for a new idea again, this time, we look at a commutator of two cycles (123) and (234) and note that it indeed permutes the four solutions since $[(123),(2,3,4)] = (14)(23)$.

- Applying $(123) = [(12),(23)]$ followed by $(234) = [(23),(34)]$ to functions of type R_1 produces two closed loops γ_1 followed by γ_2 coming back to the original position.

- However, functions of type R_2 will move along two generally unclosed paths ω_1 and ω_2.

- Second, we apply these two paths backwards, in reverse, that is, $(432) = [(43), (32)]$ and then $(321) = [(32), (21)]$. During these two, R_1 -functions will follow $\gamma_2^{-1}\gamma_1^{-1}$, i.e. the previous loops backwards. Similarly, R_2-functions will travel along $\omega_2^{-1}\omega_1^{-1}$.

- Thus, the R_1-functions follow the loop $\gamma = \gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$; and R_2functions a sequence of unclosed paths $\omega_1\omega_2\omega_1^{-1}\omega_2^{-1}$, which closes on itself by construction.

- Our conclusion has therefore been reached: while $\left(s_1, s_2, s_3, s_4\right)$ undergoes the permutation $(14)(23)$ written as a commutator of commutators, any R_2 -function follows a loop.

The quintic

- Let $p(z) = 0$, where $p(z) = z^5 + c_4 z^4 + c_3 z^3 + c_2 z^2 + c_1 z + c_0$ be the quintic equation. Suppose that

$$s_\mathrm{i} = R_{3i}\left(c_0, \ldots, c_4\right) \text{ for } i \in \{1,\ldots,5\},$$

where the functions R_{3i} has three nested levels of roots.

- Following what is done for $n = 2,3,4$, note that (1) all R_k-functions with $k = 0,1,2$, will follow a loop from a commutator of commutators of the solutions (as in the quartic case), but (2) we will need one more level of commutators for the additional root appearing in R_3.

- In general, for $n = 5$, we have $[(ijk), (k\ell m)] = (jkm)$.

- Thus, any cycle (jkm) can be written as a commutator of two other cycles, namely $[(ijk),(k\ell m)]$.

- But notice that this is true for any cycle (jkm), including (ijk) and $(k\ell m)$ on the left-hand side of the equality: $[(ijk),(k\ell m)] = (jkm)$. In other words, this formula can be applied to itself.

- Hence the cycle (jkm) can be written as a nested commutator of commutators as many as times as we want.

- Since a number $m \in \mathbb{N}$ of commutators allows us to discard precisely m levels of roots in a formula, we can actually discard any number of roots in any proposed formula for the quintic!

A short summary

Let $\mathscr{C}$ denote the space of coefficients of the quintic minus those leading to double roots. Let $\mathscr{S}$ denote the space of solutions to a quintic consisting of five distinct unordered complex numbers $\{s_1, \ldots, s_5\}$. Order these, in anyway you like when a fixed but arbitrary quintic is chosen. Suppose that a solution of the quintic equation can be expressed by a multi-valued function F.

- There is a onto map from the space of loops to the permutation group S_5.
- Suppose that $\gamma \in \pi_1(\mathscr{C})$ induces a cycle (123). Then picking a fixed branch of F, claim that $F \circ \gamma(0) = \gamma_1 = F \circ \gamma(1)$, which is a contradiction!
- The claim is easily verified by checking that (123) is a commutator of commutators in the permutation group S_5 on 5 symbols.

Paul Ramond, The Abel–Ruffini's Theorem: Complex but Not Complicated!, The American Mathematical Monthly, 129 (2022), 231-245.

LEO GOLDMAKHER, Arnold's elementary proof of the insolvabilty of the quintic

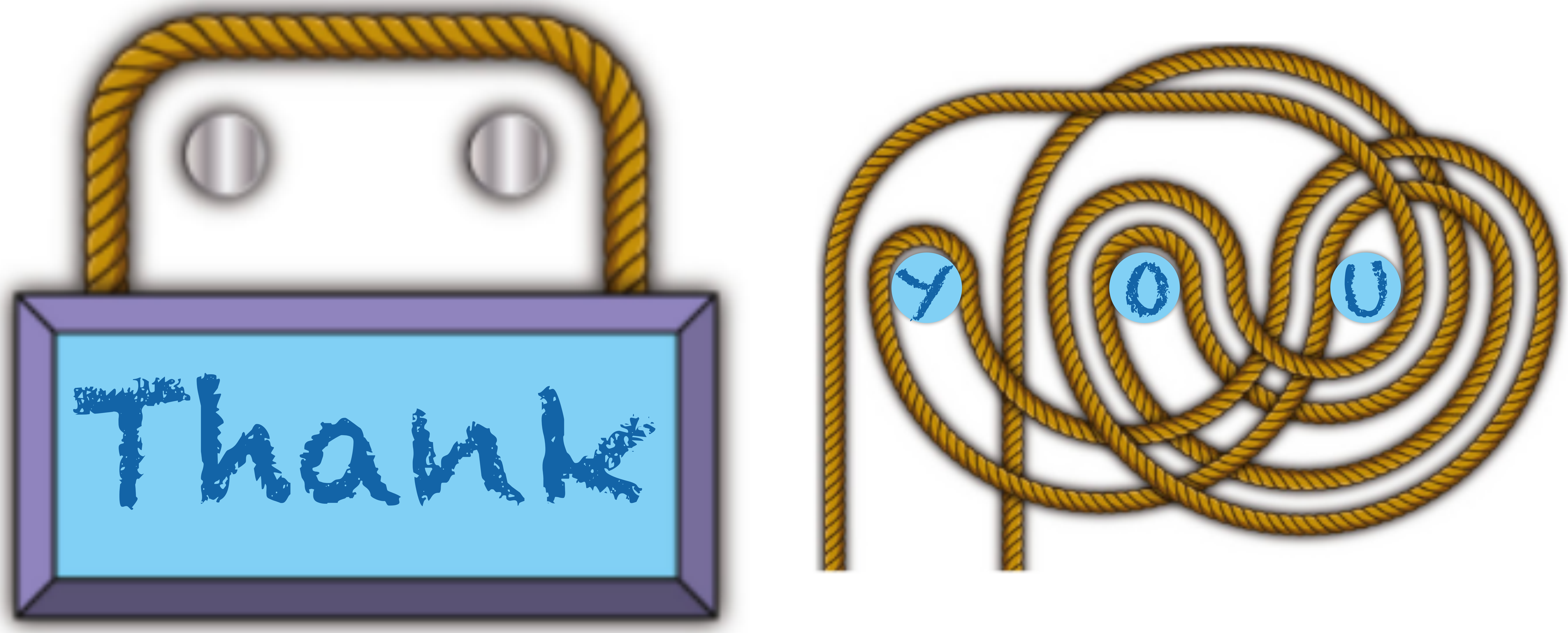
F. Akalin, Why is the Quintic Unsolvable? — akalin.com/quintic-unsolvabilityhttps://www.youtube.com/watch?v=BSHv9Elk1MU

Boaz Katz, https://www.youtube.com/watch?v=zeRXVL6qPk4&t=530s

Leo Stein, https://duetosymmetry.com/tool/polynomial-roots-toy/

Ramaprasad Saptharisi, https://www.youtube.com/watch?v=O5eH3x3sTNA

Carl Turner(Not all wrong), https://www.youtube.com/watch?v=BSHv9Elk1MU


Thank
Y O U